Claims

1. A method for handling a broadcast packet in a gateway computer (131, 132, 612, 622, 632, 711, 721, 731, 741, 1111, 1112, 1301) that has an IPsec-protected connection to a part (121, 122, 141, 732, 733, 742, 743, 1113, 1114) of a logical network segment (101, 601, 701, 1101) within which the broadcast packet should be distributed, wherein the IPsec protection specifies, what kinds of packets are acceptable for transmission over the IPsec-protected connection, **characterized** in that the method comprises the steps of:

- encapsulating (204, 311, 508, 835, 838, 840, 842, 849, 852, 909) the broadcast packet into a form that is acceptable for transmission over the IPsec-protected connection and

- transmitting (205, 206, 312, 509, 836, 839, 841, 843, 850, 853, 910) the encapsulated broadcast packet to the part of the logical network segment through the IPsec-protected connection.

2. A method according to claim 1, **characterized** in that it comprises the steps of:

- duplicating (204, 311, 508, 835, 838, 840, 842, 849, 852, 909) the broadcast packet into as many copies as there are IPsec-protected connections from the gateway computer (131, 132, 612, 622, 632, 711, 721, 731, 741, 1111, 1112, 1301) to such parts of the logical network segment (101, 601, 701, 1101) to which the broadcast packet should be transmitted, and

- repeating said encapsulating and transmitting steps in respect of every duplicated copy of the broadcast packet, so that at each repetition a duplicated copy of the broadcast packet is encapsulated into a form that is acceptable for transmission over an IPsec-protected connection to a part to which it was not yet transmitted and from which the broadcast packet was not received, and thereafter such an encapsulated broadcast packet is transmitted to such a part.

3. A method according to claim 2, **characterized** in that the step of duplicating (204, 311, 508, 835, 838, 840, 842, 849, 852, 909) the broadcast packet comprises the substeps of:

- in case there exists a bunch of currently existing IPsec-protected connections (1211, 1212, 1213, 1214) that begin at the gateway computer and end at a certain same receiving device, which is part of the logical network segment, selecting only one IPsec-protected connection from each such bunch and

- refraining from duplicating the broadcast packet into more than one copy per bunch;

so that from the gateway computer to said certain receiving device an encapsulated copy of the broadcast packet is only transmitted through the selected IPsec-protected connection.

4. A method according to claim 1, **characterized** in that comprises the steps of:
- checking (905), whether there are such unprotected connections from the gateway computer to parts of the logical network segment within which the broadcast packet should be distributed, from which unprotected connections the broadcast packet was not received to the gateway computer, and
- if such unprotected connections are found, transmitting (906) the broadcast packet as such to those unprotected connections.

5. A method according to claim 1, **characterized** in that the encapsulating step comprises adding new headers (411, 412) to the broadcast packet, which new headers include a new IP header (411) and a security header (412), of which the new IP header (411) identifies an endpoint of the IPsec-protected connection as the intended destination of the encapsulated broadcast packet and the security header (412) conforms to security features of the IPsec protection.

6. A method for transmitting a broadcast packet from a host computer (121, 122, 141, 732, 733, 742, 743, 1113, 1114, 1301), which host computer is part of a certain logical network segment (101, 601, 701, 1101) within which the broadcast packet should be distributed and has an IPsec-protected connection to another part (131, 132, 612, 622, 632, 711, 721, 731, 741, 1111, 1112) of the logical network segment, wherein the IPsec protection specifies, what kinds of packets are acceptable for transmission over the IPsec-protected connection, **characterized** in that the method comprises the steps of:
- encapsulating (504, 832) the broadcast packet into a form that is acceptable for transmission over the IPsec-protected connection and
- transmitting (505, 833) the encapsulated broadcast packet to the other part of the logical network segment through the IPsec-protected connection.

7. A method according to claim 6, **characterized** in that the encapsulating step comprises adding new headers (411, 412) to the broadcast packet, which new headers include a new IP header (411) and a security header (412), of which the new IP header (411) identifies an endpoint of the IPsec-protected connection as the intended destination of the encapsulated broadcast packet and the security header (412) conforms to security features of the IPsec protection.

8. A method according to claim 6, **characterized** in that the step of encapsulating the broadcast packet comprises the substeps of:
- in case there exists a bunch of currently existing IPsec-protected connections (1211, 1212, 1213, 1214) that begin at the host computer and end at a certain same receiving device, which is part of the logical network segment, selecting only one IPsec-protected connection from such bunch and
- encapsulating the broadcast packet into a form that is acceptable for transmission over just the selected IPsec-protected connection.

9. A method for conveying a broadcast packet from a first part (102, 611, 621, 623, 710, 720, 730, 740, 1101) of a logical network segment (101, 601, 701, 1101), within which the broadcast packet should be distributed, to a second part (102, 611, 621, 623, 710, 720, 730, 740, 1101) of the same logical network segment that has an IPsec-protected connection to the first part, wherein the IPsec protection specifies, what kinds of packets are acceptable for transmission over the IPsec-protected connection, **characterized** in that the method comprises the steps of:
- encapsulating (204, 311, 504, 508, 832, 835, 838, 840, 842, 849, 852, 909) the broadcast packet within the first part of the logical network segment into a form that is acceptable for transmission over the IPsec-protected connection,
- transmitting (205, 206, 312, 505, 509, 833, 836, 839, 841, 843, 850, 853, 910) the encapsulated broadcast packet to the second part of the logical network segment through the IPsec-protected connection and
- decapsulating (506, 844, 846, 851, 854) the transmitted encapsulated broadcast packet at the second part of the logical network segment.

10. A gateway computer (131, 132, 612, 622, 632, 711, 721, 731, 741, 1111, 1112, 1301) for offering another computer device an IPsec-protected connection to and from a logical network segment (101, 601, 701, 1101) within which the distribution of broadcast packets is allowable, wherein the IPsec protection is arranged to specify, what kinds of packets are acceptable for transmission over an IPsec-protected connection, **characterized** in that the gateway computer comprises:
- means (1311, 1321) for encapsulating a broadcast packet into a form that is acceptable for transmission over an IPsec-protected connection and
- means (1312, 1322) for transmitting the encapsulated broadcast packet to the other computer device through an IPsec-protected connection.

11. A gateway computer according to claim 10, **characterized** in that it comprises:

- a first network interface (1322) for connecting the gateway computer to a logical network segment comprising several computer devices,
- a second network interface (1312) for connecting the gateway computer to individual hosts for the purpose of making such individual hosts appear as parts of the logical network segment,
- an IPsec component (1311) coupled to the second network interface (1312) for implementing IPsec protection within connections through said second network interface, and
- a broadcast packet handler component (1350);

wherein the broadcast packet handler component is arranged to:

- receive (1355) broadcast packets from either of the first (1322) and second (1312) network interfaces,
- forward (1353) received broadcast packets to application layer entities (1302) in the gateway computer,
- forward (1353) broadcast packets received from the first network interface (1322) towards the second network interface (1312),
- forward (1353) broadcast packets received from the second network interface (1312) towards the first network interface (1322),
- forward (1353) broadcast packets from application layer entities (1302) in the gateway computer towards the first and second network interfaces, and
- instruct the IPsec component (1311) regarding protected transmission of broadcast packets through the second network interface.

12. A gateway computer according to claim 11, **characterized** in that the broadcast packet handler component (1350) is additionally arranged to receive information (1355) from the IPsec component (1311) regarding the number and endpoints of currently existing IPsec-protected connections through the second network interface.

13. A host computer (121, 122, 141, 732, 733, 742, 743, 1113, 1114, 1301), comprising means (1311, 1312) for establishing an IPsec-protected connection to and from a gateway computer of a logical network segment within which the distribution of broadcast packets is allowable, wherein the IPsec protection is arranged to specify, what kinds of packets are acceptable for transmission over the IPsec-protected connection, **characterized** in that the host computer comprises:

- means (1311) for encapsulating a broadcast packet into a form that is acceptable for transmission over the IPsec-protected connection and
- means (1312) for transmitting the encapsulated broadcast packet to the gateway computer through the IPsec-protected connection.

14. A host computer according to claim 13, **characterized** in that it comprises:
- a network interface (1312) for connecting the host computer to a gateway computer,
- an IPsec component (1311) coupled to the network interface (1312) for implementing IPsec protection within connections through said network interface, and
- a broadcast packet handler component (1350);
wherein the broadcast packet handler component is arranged to:
- receive (1355) broadcast packets from the network interface,
- forward (1353) received broadcast packets to application layer entities (1302) in the host computer,
- forward (1353) broadcast packets from application layer entities (1302) in the host computer towards the network interface (1312), and
- instruct the IPsec component (1311) regarding protected transmission of broadcast packets through the network interface.

15. A gateway computer according to claim 14, **characterized** in that the broadcast packet handler component (1350) is additionally arranged to receive (1355) information from the IPsec component (1311) regarding the number and endpoints of currently existing IPsec-protected connections through the network interface.

16. A computer program product comprising a computer readable medium, having thereon: computer program code means, when said program is loaded, to make the computer execute procedures to encapsulate a broadcast packet into a form that is acceptable for transmission over an IPsec-protected connection; and transmit the encapsulated broadcast packet a part of a logical network segment different than the computer itself through an IPsec-protected connection.

17. A computer program element comprising: computer program code means to make the computer execute a procedure to encapsulate a broadcast packet into a form that is acceptable for transmission over an IPsec-protected connection; and

transmit the encapsulated broadcast packet a part of a logical network segment different than the computer itself through an IPsec-protected connection.

18. A computer program element as claimed in claim 17 embodied on a computer readable medium.

19. A computer readable medium, having a program recorded thereon, where the program is to make the computer execute procedures to encapsulate a broadcast packet into a form that is acceptable for transmission over an IPsec-protected connection; and transmit the encapsulated broadcast packet a part of a logical network segment different than the computer itself through an IPsec-protected connection.

20. A computer program product directly loadable into the internal memory of a digital computer, comprising software code portions for performing the steps of claim 19 when said product is run on a computer.

21. A computer program product stored on a computer usable medium, comprising: computer readable program means for causing a computer to perform the steps of claim 19 when said product is run on a computer.